HIPAA PRIVACY

Overview

Office for Civil Rights

Department of Health and Human Services

February 9, 2003

Privacy Rule Process

- Final Rule published 12/28/00
- Final modifications published 8/14/02
- Compliance by 4/14/03 for most covered entities

Outline of Privacy Rule

- Who and what is covered
- Uses and disclosures of protected health information
- Individual rights
- Administrative provisions
- Organizational Issues
- Compliance and enforcement

Scope: Who is Covered?

- Limited by HIPAA to:
  - Health care providers who transmit health information electronically in connection with a transaction for which there is a HIPAA standard
  - Health plans
  - Health care clearinghouses
- Business associate relationships

Business Associates

- Agents, contractors, others hired to do work of or for covered entity that requires use or disclosure of protected health information
- Require satisfactory assurance – usually a contract – that a business associate will safeguard protected health information, limit use and disclosure

Scope: What is Covered?

- Protected health information (PHI) is:
  - Individually identifiable health information
  - Transmitted or maintained in any form or medium by covered entities or their business associates (includes oral, paper, and electronic)
- De-identified information is not covered
- Employment and FERPA (Family Educational Rights & Privacy Act) records are not covered

Uses & Disclosures: Key Points

- NO use or disclosure of PHI unless required or permitted by the Rule
- Required disclosures are limited to:
  - Disclosures to the individual who is the subject of information
  - Disclosures to Secretary of HHS to determine compliance
- All other uses & disclosures in Rule are permissive
- Covered entities can provide greater protections

Permissive Uses & Disclosures

- To the individual (or personal representative)
- For treatment, payment, & health care operations (TPO)
- Opportunity to agree or object
- For specific public priorities
- “Incident To”
- Limited Data Set
- As authorized by the individual

To Individuals

Besides required disclosures, covered entities also may disclose PHI to their patients/health plan enrollees Examples:

- Health plans can contact their enrollees
- Providers can talk to their patients

Treatment, Payment and Health Care Operations (TPO)

Covered entity may use/disclose PHI to carry out essential health care functions

- Treatment
- Payment
- Health care operations

Opportunity to Agree or Object

- Facility directories (name, location, general condition, clergy – religious affiliation)
- To persons involved in care or payment for care and for notification purposes
    - Friends can pick up prescriptions
    - Hospitals can notify family members of patient's condition
    - Covered entities can notify disaster relief agencies

Public Policy Purposes

(a) As required by law

(b) For public health

(c) About victims of abuse, neglect or domestic violence

(d) For health oversight activities

(e) For judicial & administrative proceedings

(f) For law enforcement purposes

Public Policy Purposes (2)

(g) About decedents (to coroners, medical examiners, funeral directors)

(h) For cadaveric organ, eye or tissue donations

(i) For certain research

(j) To avert a serious threat to health or safety

(k) For specialized government functions (military, veterans, national security, protective services, State Dept., correctional facilities)

(l) For workers' compensation

"Incident to" Uses and Disclosures

- Rule permits uses/disclosures incident to an otherwise permitted use or disclosure, provided minimum necessary & safeguards standards are met
- Allows for common practices if reasonably performed

Limited Data Set

- For research, public health, health care operations purposes
- Direct identifiers must be removed
- Allows zip codes, dates
- Requires Data Use Agreement: recipient cannot use for other purposes or identify or contact individuals

Uses/Disclosures Requiring Authorization

Authorizations are required for uses and disclosures not otherwise permitted or required by the Rule

Authorization

- Generally, cannot condition treatment, payment, eligibility, or enrollment on an authorization
- Special rules:
  - psychotherapy notes
  - marketing
- Authorization must contain core elements & required statements, including:
  - Expiration Date or event
  - Statement that authorization is revocable

Minimum Necessary

Covered entities must make reasonable efforts to limit the use or disclosure of, and requests for, PHI to minimum amount necessary to accomplish intended purpose

Minimum Necessary Policies & Procedures for Uses, Disclosures, Requests

- **Uses**
  - Role-based access
- **Disclosures & Requests**
  - Standard protocols for routine/recurring
  - Case-by-case review for non-routine
- **Reasonable Reliance**

Minimum Necessary Exceptions

- Disclosures to or requests by providers for treatment
- Disclosures to individual
- Uses/disclosures with an authorization
- Uses/disclosures required for HIPAA standard transaction
- Disclosures to HHS/OCR for enforcement
- Uses/disclosures required by law

Individual's Rights

Individuals have the right to:

- A written notice of privacy practices from covered entities with specific delivery requirements for health plans and providers
  - Good faith acknowledgment
  - Exception for emergency situations
- Inspect and obtain a copy of their PHI

Individual's Rights (cont.)

Individuals have the right to:

- Obtain an accounting of disclosures
- Amend their records
- Request restrictions on uses and disclosures
- Accommodation of reasonable communication requests
- Complain to the covered entity and to HHS

Administrative Requirements

Flexible & scalable

- Covered entities required to:
  - Designate a privacy official and contact person
  - Develop policies and procedures (including for receiving complaints)
  - Provide privacy training to its workforce
  - Implement administrative, technical, and physical safeguards

Administrative Requirements (cont.)

- Develop a system of sanctions for employees
- Meet documentation requirements
- Mitigate any harmful effect of a use or disclosure of protected health information that is known to the covered entity
- Refrain from intimidating or retaliatory acts
- Not require individuals to waive their rights to file a complaint with the Secretary or their other rights under this Rule

Organizational Issues

- Hybrid Entities
- Organized Health Care Arrangements (OHCAs)
- Affiliated Covered Entities

Hybrid Entities

- Covered entity that also does non-covered functions may choose to be hybrid entity and designate health care component(s)
- Hybrid entity must ensure health care component complies w/requirements of Rule
- Sharing of PHI between health care and non-health care components is a disclosure – allowed only to same extent permitted to a separate entity

OHCAs and Affiliated Covered Entities

- OHCA
  - Special arrangement whereby multiple covered entities can share PHI
    - E.g., clinically integrated care settings
  - Joint notice permitted

- Affiliated Covered Entities
  - Legally separate covered entities that are affiliated (under common ownership and control) may choose to be treated as a single covered entity

Compliance and Enforcement

- Technical assistance for voluntary compliance
- Any person or organization can file complaints with OCR (generally within 180 days)
- OCR may investigate complaints and may conduct compliance reviews
- OCR shall attempt to resolve noncompliance by informal means

Technical Assistance

- Integrated Rule and Preambles to Dec. 2000, Aug. 2002 Final Rules
- Covered Entity decision tool
- December 4, 2002 Guidance
- Targeted Technical Assistance materials under development
- Fact sheet on August 2002 modifications
- Sample Business Associate Contract
- FAQs on our website
- http://www.hhs.gov/ocr/hipaa/

Compliance and Enforcement: Civil Monetary Penalties (CMPs)

- Civil monetary penalties can be imposed by OCR
  - $100 per violation
  - Capped at $25,000 for each calendar year for each requirement or prohibition that is violated

Compliance and Enforcement: Criminal Penalties

- Criminal penalties
  - Up to $50,000 & 1 year imprisonment for knowingly obtaining or disclosing IIHI in violation of HIPAA rules
  - Up to $100,000 & 5 years if done under false pretenses
  - Up to $250,000 & 10 years if done with intent to sell, transfer, or use for commercial advantage, personal gain or malicious harm
- Enforced by DOJ

OCR Web Site and Telephone Number

www.hhs.gov/ocr/hipaa

(866) 627-7748